



Permisos de seguridad de archivos

ONTAP Automation

NetApp
July 11, 2024

Tabla de contenidos

- Permisos de seguridad de archivos 1
 - Prepárese para gestionar la seguridad de archivos y las políticas de auditoría 1
 - Obtenga los permisos efectivos para un archivo 2
 - Obtener la información de auditoría de un archivo 3
 - Aplicar nuevos permisos a un archivo 6
 - Actualice la información del descriptor de seguridad 7
 - Eliminar una entrada de control de acceso 8

Permisos de seguridad de archivos

Prepárese para gestionar la seguridad de archivos y las políticas de auditoría

Puede gestionar los permisos y las políticas de auditoría para los archivos disponibles a través de las máquinas virtuales de almacenamiento en un clúster de ONTAP.

Descripción general

ONTAP utiliza las listas de control de acceso del sistema (SACL) y las listas de control de acceso discrecional (DACL) para asignar permisos a los objetos de archivo. A partir de ONTAP 9,9.1, la API DE REST incluye soporte para gestionar los permisos SACL y DACL. Puede utilizar la API para automatizar la administración de los permisos de seguridad de archivos. En muchos casos, puede usar una sola llamada a la API DE REST en lugar de varios comandos de la CLI o llamadas a ONTAPI (ZAPI).



Para versiones de ONTAP anteriores a 9,9.1, puede automatizar la administración de los permisos SACL y DACL mediante la función de paso de CLI. Consulte ["Consideraciones sobre migración"](#) y.. ["Utilizando el traspaso de interfaz de línea de comandos privada con la API REST de ONTAP"](#) si quiere más información.

Hay varios ejemplos de flujos de trabajo disponibles para ilustrar cómo se gestionan los servicios de seguridad de archivos ONTAP mediante la API de REST. Antes de usar los flujos de trabajo y emitir alguna de las llamadas a la API DE REST, asegúrese de revisarlos ["Prepárese para usar los flujos de trabajo"](#).

Si usas Python, también consulta el script ["file_security_permissions.py"](#) para obtener ejemplos de cómo automatizar algunas de las actividades de seguridad de archivos.

API REST de ONTAP frente a comandos de la CLI de ONTAP

En muchas tareas, el uso de la API DE REST DE ONTAP requiere menos llamadas que los comandos equivalentes de la CLI de ONTAP o llamadas a ONTAPI (ZAPI). La siguiente tabla incluye una lista de llamadas API y el equivalente a los comandos CLI necesarios para cada tarea.

API REST de ONTAP	CLI de ONTAP
GET /protocols/file-security/effective-permissions/	<code>vserver security file-directory show-effective-permissions</code>
POST /protocols/file-security/permissions/	<ol style="list-style-type: none"><code>vserver security file-directory ntfs create</code><code>vserver security file-directory ntfs dacl add</code><code>vserver security file-directory ntfs sacl add</code><code>vserver security file-directory policy create</code><code>vserver security file-directory policy task add</code><code>vserver security file-directory apply</code>

API REST de ONTAP	CLI de ONTAP
PATCH /protocols/file-security/permissions/	vserver security file-directory ntfs modify
DELETE /protocols/file-security/permissions/	<ol style="list-style-type: none"> 1. vserver security file-directory ntfs dacl remove 2. vserver security file-directory ntfs sacl remove

Información relacionada

- ["Script de Python que ilustra los permisos de archivo"](#)
- ["Gestión simplificada de permisos de seguridad de archivos con API DE REST de ONTAP"](#)
- ["Utilizando el traspaso de interfaz de línea de comandos privada con la API REST de ONTAP"](#)

Obtenga los permisos efectivos para un archivo

Puede recuperar los permisos efectivos actuales para un archivo o carpeta específicos.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/protocols/file-security/effective-permissions/{svm.uuid}/{path}

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligato	Descripción
\$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene el archivo.
RUTA_FILE	Ruta	Sí	Esta es la ruta al archivo o carpeta.

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/protocols/file-security/effective-permissions/$SVM_ID/$FILE_PATH" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON

```
{
  "svm": {
    "uuid": "cf5f271a-1beb-11ea-8fad-005056bb645e",
    "name": "vs1"
  },
  "user": "administrator",
  "type": "windows",
  "path": "/",
  "share": {
    "path": "/"
  },
  "file_permission": [
    "read",
    "write",
    "append",
    "read_ea",
    "write_ea",
    "execute",
    "delete_child",
    "read_attributes",
    "write_attributes",
    "delete",
    "read_control",
    "write_dac",
    "write_owner",
    "synchronize",
    "system_security"
  ],
  "share_permission": [
    "read",
    "read_ea",
    "execute",
    "read_attributes",
    "read_control",
    "synchronize"
  ]
}
```

Obtener la información de auditoría de un archivo

Puede recuperar la información de auditoría de un archivo o carpeta específicos.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/protocols/file-security/permissions/{svm.uuid}/{path}

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
\$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene el archivo.
RUTA_FILE	Ruta	Sí	Esta es la ruta al archivo o carpeta.

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON

```
{
  "svm": {
    "uuid": "9479099d-5b9f-11eb-9c4e-0050568e8682",
    "name": "vs1"
  },
  "path": "/parent",
  "owner": "BUILTIN\\Administrators",
  "group": "BUILTIN\\Administrators",
  "control_flags": "0x8014",
  "acls": [
    {
      "user": "BUILTIN\\Administrators",
      "access": "access_allow",
      "apply_to": {
        "files": true,
        "sub_folders": true,
        "this_folder": true
      },
      "advanced_rights": {
        "append_data": true,
```

```

    "delete": true,
    "delete_child": true,
    "execute_file": true,
    "full_control": true,
    "read_attr": true,
    "read_data": true,
    "read_ea": true,
    "read_perm": true,
    "write_attr": true,
    "write_data": true,
    "write_ea": true,
    "write_owner": true,
    "synchronize": true,
    "write_perm": true
  },
  "access_control": "file_directory"
},
{
  "user": "BUILTIN\\Users",
  "access": "access_allow",
  "apply_to": {
    "files": true,
    "sub_folders": true,
    "this_folder": true
  },
  "advanced_rights": {
    "append_data": true,
    "delete": true,
    "delete_child": true,
    "execute_file": true,
    "full_control": true,
    "read_attr": true,
    "read_data": true,
    "read_ea": true,
    "read_perm": true,
    "write_attr": true,
    "write_data": true,
    "write_ea": true,
    "write_owner": true,
    "synchronize": true,
    "write_perm": true
  },
  "access_control": "file_directory"
}
],
"inode": 64,

```

```

"security_style": "mixed",
"effective_style": "ntfs",
"dos_attributes": "10",
"text_dos_attr": "----D---",
"user_id": "0",
"group_id": "0",
"mode_bits": 777,
"text_mode_bits": "rwxrwxrwx"
}

```

Aplicar nuevos permisos a un archivo

Puede aplicar un nuevo descriptor de seguridad a un archivo o carpeta específicos.

Paso 1: Aplique los nuevos permisos

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/protocols/file-security/permissions/{svm.uuid}/{path}

Tipo de procesamiento

Asíncrona

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
\$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene el archivo.
RUTA_FILE	Ruta	Sí	Esta es la ruta al archivo o carpeta.

Ejemplo de curl

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{ \acl\": [ { \access\": \access_allow\", \advanced_rights\": { \append_data\": true, \delete\": true, \delete_child\": true, \execute_file\": true, \full_control\": true, \read_attr\": true, \read_data\": true, \read_ea\": true, \read_perm\": true, \write_attr\": true, \write_data\": true, \write_ea\": true, \write_owner\": true, \write_perm\": true }, \apply_to\": { \files\": true, \sub_folders\": true, \this_folder\": true }, \user\": \administrator\" } ], \control_flags\": \32788\", \group\": \S-1-5-21-2233347455-2266964949-1780268902-69700\", \ignore_paths\": [ \parent/child2\" ], \owner\": \S-1-5-21-2233347455-2266964949-1780268902-69304\", \propagation_mode\": \propagate\''
```

Ejemplo de resultado JSON

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Paso 2: Recuperar el estado del trabajo

Realice el flujo de trabajo ["Obtener instancia de trabajo"](#) y confirme el `state` el valor es `success`.

Actualice la información del descriptor de seguridad

Puede actualizar un descriptor de seguridad específico a un archivo o carpeta específicos, incluidos los indicadores de propietario, grupo o control principal.

Paso 1: Actualice el descriptor de seguridad

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PARCHE	/api/protocols/file-security/permissions/{svm.uuid}/{path}

Tipo de procesamiento

Asíncrona

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
\$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene el archivo.
RUTA_FILE	Ruta	Sí	Esta es la ruta al archivo o carpeta.

Ejemplo de curl

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{ \"control_flags\": \"32788\", \"group\": \"everyone\", \"owner\": \"user1\"}'
```

Ejemplo de resultado JSON

```
{
  "job": {
    "uuid": "6f89e612-5bbd-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/6f89e612-5bbd-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Paso 2: Recuperar el estado del trabajo

Realice el flujo de trabajo ["Obtener instancia de trabajo"](#) y confirme el state el valor es success.

Eliminar una entrada de control de acceso

Puede eliminar una entrada de control de acceso (ACE) existente de un archivo o carpeta específicos. El cambio se propaga a cualquier objeto secundario.

Paso 1: Eliminar el ACE

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
ELIMINAR	/api/protocols/file-security/permissions/{svm.uuid}/{path}

Tipo de procesamiento

Asíncrona

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligato	Descripción
\$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene el archivo.
RUTA_FILE	Ruta	Sí	Esta es la ruta al archivo o carpeta.

Ejemplo de curl

```
curl --request DELETE --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{ "access": "access_allow", "apply_to": { "files": true, "sub_folders": true, "this_folder": true }, "ignore_paths": [ "/parent/child2" ], "propagation_mode": "propagate" }'
```

Ejemplo de resultado JSON

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Paso 2: Recuperar el estado del trabajo

Realice el flujo de trabajo ["Obtener instancia de trabajo"](#) y confirme el `state` el valor es `success`.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.